MacWilliams Identites for Linear Codes with Group Action(Algebraic Combinatorial Theory)

AUTHOR(S):

YOSHIDA, TOMOYUKi

CITATION:

YOSHIDA, TOMOYUKi. MacWilliams Identites for Linear Codes with Group Action(Algebraic Combinatorial Theory). 数理解析研究所講究録 1988, 671: 33-54

ISSUE DATE:

1988-09

URL:

http://hdl.handle.net/2433/100825

数理解析研究所講究録
第 671 巻 1988 年 33-54

MacWilliams Identities for Linear Codes with Group Action

TOMOYUKI YOSHIDA

Dept. of Math. Hokkaido Univ.

CONTENTS.

1. Codes.
2. We work in the category of G-sets.
3. How to define equivariant weight enumerators.
4. The equivariant MacWilliams identity.
5. The outline of the proof.
6. A weight enumerator is an invariant polynomial.
7. Numerical examples.
8. Problems.

1. CODES

First of all, we introduce notation and terminology in coding theory. Let $F := GF(q)$ be the Galois field of order q, $N := \{1, \ldots, n\}$, and $V := F^N := \{v : N \longrightarrow F\}$, so that V can be identified as the row vector space of dimension n. The **support** and the **weight** of a vector $v \in V$ are defined by

$$\mathrm{supp}(v) := \{i \in N \mid v_i \neq 0\},$$

$$|v| := \mathrm{wt}(v) := |\mathrm{supp}(v)|.$$

Furthermore V has an usual inner product

$$\langle u, v \rangle := \sum_{i=1}^{n} u_i v_i.$$

Now a **code** C of **length** n is a subspace of V. The **minimal distance**(or **minimal weight**) of the code C is defined by

$$d(C) := \min\{\, |u| \mid 0 \neq u \in C \,\}$$

The **dual code** of C is the orthogonal complement

$$C^{\perp} := \{\, v \in V \mid \langle u, v \rangle = 0 \qquad \forall u \in C \,\}.$$

The code C is called to be **self-dual** if $C^{\perp} = C$.

The **weight enumerator** is the homogeneous polynomial of degree n defined by

$$w_C(x, y) := \sum_{u \in C} x^{n-|u|} y^{|u|} := \sum_{r=0}^{n} A_r x^{n-r} y^r,$$

where $\{\, A_1, \ldots, A_n \,\}$ is the **weight distribution** of C, that is,

$$A_r := \sharp\{\, u \in C \mid |u| = r \,\}.$$

Then the **MacWilliams identity** holds:

THEOREM 1.1 (MACWILLIAMS).

$$w_{C^{\perp}}(x, y) = \frac{1}{|C|} w_C(x + (q-1)y, x - y).$$

For the detail, refer to [MS77], [Pl82], [MMS72].

The purpose of this paper is to extend this identity to codes with group actions.

2. We work in the category of G-sets

Throughout this section G denotes a finite group. A G-set X is a set equipped with right G-action

$$X \times G \longrightarrow X\,;\,(x,\sigma) \mapsto x\sigma.$$

A G-map $f : X \longrightarrow Y$ between G-sets is a map of X to Y such that $f(x\sigma) = f(x)\sigma$.

Let $\mathbf{Set}^G$ denote the category of G-sets and G-maps; and let $\mathbf{Set}_f^G$ denote the category of finite G-sets. If we consider combinatorial theory as a theory of $\mathbf{Set}_f$, the category of finite sets, then the theory of $\mathbf{Set}_f^G$ can be consider as equivariant combinatorial theory. I have studied Fisher's inequality for block designs with group action based on this idea([Yo87]). Fortunately, this idea can be also applied to the formulation and the proof of the MacWilliams identity for linear codes with group action.

Because the category of G-sets has similar properties as the category of sets, we can formally extend usual theories to theories with group action: that is, equivariant versions of theories. However the category of G-sets has many non-isomorphic connected objects (transitive G-sets) in addition to the terminal object, if G is not trivial. For this reason, it is often unavoidable that such theories become too difficult to study them directly. For example, the theory of vector spaces is easy, but the theory of vector spaces with group action is nothing but the representation theory of groups. Even the definition of the concept of matrices is not trivial in this theory.

Now, for two G-sets X and Y, we use the following notation:

$$X + Y : \text{ disjoint union;}$$

$$X \times Y : \text{ direct product;}$$

$$Y^X := \{ f : X \longrightarrow Y \} : \text{ configuration set;}$$

where the G-action on Y^X is defined by

$$f^\sigma(x) := f(x\sigma^{-1}) \cdot \sigma \qquad \text{for } f \in Y^X, \sigma \in G, x \in X.$$

For example, when G acts on $N := \{1, \cdots, n\}$ and F is the field with q elements, the row vector space $V := F^N$ becomes a G-module by this way. The action of G on F is supposed to be trivial. The power set 2^X of a G-set becomes also a G-set in the usual way. Furthermore, the one point set, denoted by $\mathbf{1}$, is a terminal object of $\mathbf{Set}^G$.

Next, let X be a G-set and H a subgroup of G. Then we obtain the H-fixed point set and the H-orbit set:

$$X^H := \{ x \in X \mid xh = x \quad \forall h \in H \};$$

$$X/H := \{ xH \mid x \in X \}.$$

(Be careful not to confuse X^H and Y^X.) For example, for the row vector space $V := F^N$ as above, V^H is canonically isomorphic to $F^{N/H}$. Thus if C is an FG-subspace (=G-code) of V, then C^H can be regarded as a subspace (= code) of $F^{N/H}$.

The disjoint union $X + Y$ and the direct product $X \times Y$ of finite G-sets satisfies the distributive law, and so the isomorphism classes of finite

G-sets make a semi-ring. Thus the **Burnside ring** $\Omega(G)$ is defined as the Grothendieck ring of $\mathbf{Set}_f^G$ with respect to disjoint unions and direct products, that is, $\Omega(G)$ is generated by $[X]$, $X \in \mathbf{Set}_f^G$ and has the relations

$$[X] = [Y], \text{ if } X \cong_G Y,$$
$$[X + Y] = [X] + [Y].$$

Since any finite G-set splits uniquely into a disjoint union of transitive G-sets, we see that $\Omega(G)$ is a free abelian group with basis $\{\, [H\backslash G] \mid (H) \in C(G) \,\}$, where $C(G)$ is the set of the G-conjugacy classes (H) of subgroups $H \leq G$. The Burnside ring plays a role as the ring of "integers" in equivariant theories.

For any subgroup H of G, the map $[X] \mapsto |X^H|$ can be extended to a ring homomorphism $\varphi_H : \Omega(G) \longrightarrow \mathbb{Z}$. Taking the product of φ_H for all conjugacy classes $(H) \in C(G)$, we have a ring homomorphism

$$\varphi := \prod \varphi_H : \Omega(G) \longrightarrow \widetilde{\Omega}(G) := \prod_{(H)\in C(G)} \mathbb{Z}.$$

The following lemma is the fundamental theorem for Burnside rings and it is due essentially to Burnside (cf. [Bu11]):

LEMMA 2.1. *$\varphi : \Omega(G) \longrightarrow \widetilde{\Omega}(G)$ is an injective ring homomorphism and its cokernel is isomorphic to $\prod_{(H)}(\mathbb{Z}/|N_G(H) : H|\,\mathbb{Z})$.*

There are **congruence relations** which characterize the image of φ. See tom Dieck's book [Di79].

Any G-set Z can be regarded as a category as follows:

$$\mathrm{Obj}(Z) := Z;$$
$$\hom_Z(x,y) := \{\, \sigma \in G \mid x = y\sigma \,\}.$$

The compositions are defined by multiplication in the group G.

Let Z be a finite G-set. We view Z as a category. A functor $Z^{\mathrm{op}} \longrightarrow \mathbf{Set}_f$ is called a **finite set over Z**, where Z^{op} is the dual category. Thus a finite set A over Z consists of finite sets $A(z), z \in Z$ and isomorphisms between finite sets $\sigma^* : A(z) \overset{\cong}{\longrightarrow} A(z\sigma); a \mapsto a\sigma$ satisfying the condition that $a1 = a, a(\sigma\tau) = (a\sigma)\tau$. Furthermore, the total space $\widetilde{A} := \coprod_{z\in Z} A(z)$ has the structure of finite G-set together with G-map $A \longrightarrow Z$. Hence $[Z^{\mathrm{op}}, \mathbf{Set}_f]$, the category of finite sets over Z, is equivalent to the comma category $\mathbf{Set}_f^G/Z$ by $A \mapsto (\widetilde{A} \longrightarrow Z)$.

LEMMA 2.2. *Let Z be a finite G-set. Two finite G-sets A, B over Z are isomorphic in the category $[Z^{\mathrm{op}}, \mathbf{Set}_f]$ if and only if $|A(z)^H| = |B(z)^H|$ for any $H \leq G$ and any $z \in Z^H$.*

This is proved by the similar way as the proof of the injectivity of φ in Lemma 2.1. Or it is proved by reducing the proof to the case where $Z \cong H\backslash G$ and by using Lemma 2.1 to H.

Furthermore, we can define , for example, an **A-module over Z** as a functor $Z^{\mathrm{op}} \longrightarrow \mathbf{Mod}_A$, where A is a ring and $\mathbf{Mod}_A$ is the category of (finitely generated) A-modules.

LEMMA 2.3(MASCHKE THEOREM). *Let Z be a finite G-set. Assume that $|G|$ is prime to the characteristic of the field F. Then the Maschke theorem holds in the category $[Z^{\mathrm{op}}, \mathbf{Mod}_F]$ of F-modules over Z.*

PROOF: For any finite G-set Z, we put $Z\hat{}:= [Z^{\mathrm{op}}, \mathbf{Mod}_F]$. Then there is a canonical equivalence of categories : $(X+Y)\hat{}\cong X\hat{}\times Y\hat{}$. Furthermore, for any transitive G-set $H\backslash G$, we have that the category $(H\backslash G)\hat{}$ is equivalent to $\mathbf{Mod}_{FH}$, the category of FH-modules. Thus the lemma follows from the ordinary Maschke theorem.

3. HOW TO DEFINE (EQUIVARIANT) WEIGHT ENUMERATORS

In this section, we define the weight enumerator of linear codes with group action. From now on, let G be a permutation group on $N := \{1, \cdots, n\}$ and let $F := GF(q)$. Then the row vector space $X := F^N$ is an FG-module. In fact, the action of G is defined by

$$(v^\sigma)_i := v_{i\sigma^{-1}} \qquad \text{for all } v \in V, \sigma \in G, i \in N.$$

The support map

$$\mathrm{supp} : V \longrightarrow 2^N ; v \mapsto \mathrm{supp}(v) \subseteq N$$

is a G-map.

A **G-code** is an FG-subspace of V. (We don't treat monomial action.) If C is a G-code, then the dual code $C^\perp$ is also a G-code.

DEFINITION. Let C be a G-code in $V := F^N$. Then the **(equivariant) weight enumerator** of C is defined by the set

$$W_C[X,Y] := \{\,(u,\rho) \in C \times (X+Y)^N \mid \mathrm{supp}(u) = \rho^{-1}(Y)\,\},$$

where X, Y are finite G-sets.

We list some properties of this weight enumerator $W_C[X,Y]$.

(1) $W_C[X,Y]$ is a G-subset of the G-set $C \times (X+Y)^N$. Furthermore, there is a pull-back diagram in $\mathbf{Set}_f^G$ as follows:

$$\begin{array}{ccc} W_C[X,Y] & \longrightarrow & C \\ \downarrow & & \downarrow{\scriptstyle \mathrm{supp}} \\ (X+Y)^N & \longrightarrow & 2^N, \end{array}$$

where the G-map $(X+Y)^N \longrightarrow 2^N$ is defined by $\rho \mapsto \rho^{-1}(Y)$.

(2) $W_C[X,Y]$ is a homogeneous polynomial of "degree N". This means that $\varphi_H(W_C[X,Y])$ is represented by a polynomial in variables $|X^D|, |Y^D|$ for all H and $D \leq G$ and that $W_C[A \times X, A \times Y] \cong_G A^N \times W_C[X,Y]$.

(3) $|W_C[X,Y]| = w_C(|X|, |Y|)$, where $w_C(x,y)$ is the ordinary weight enumerator.

(4) The equivariant weight enumerators gives a homogeneous polynomial functor of "degree N"

$$W_C : \mathbf{Set}_f^G \times \mathbf{Set}_f^G \longrightarrow \mathbf{Set}_f^G ;\ (X,Y) \mapsto W_C[X,Y].$$

Thus W_C can be extend to a polynomial map

$$W_C : \Omega(G) \times \Omega(G) \longrightarrow \Omega(G).$$

Furthermore, by the fundamental theorem of Burnside rings, it is possible to extend this map to

$$W_C : \widetilde{\Omega}(G) \times \widetilde{\Omega}(G) \longrightarrow \widetilde{\Omega}(G).$$

(5) $W_C[X, \emptyset] \cong_G X^N, W_C[\mathbf{1}, \mathbf{1}] \cong_G C$ as G-sets, where $\mathbf{1}$ is the one point set.

(6) The linear map

$$F^{N/G} \longrightarrow V^G ; (v_{iG})_{iG} \mapsto (v_{iG})_i$$

is an F-isomorphism. Thus there is a subspace D of $F^{N/G}$ corresponding to C^G. This subspace D is the **contracted code**. The (ordinary) weight enumerator $w_D(a, b)$ of D is given by

$$w_D(a, b) = \varphi_G W_C[a, b].$$

4. The equivariant MacWilliams identity

In this section, we state the MacWilliams identity for codes with group action, that is, the equivariant MacWilliams identity. As before, we assume that G acts on $N := \{1, \cdots, n\}$ and that C is a G-code in the row vector space $V := F^N$ over $F := GF(q)$.

Theorem 4.1 (Equivariant MacWilliams identity). *Assume that* $(|G|, q) = 1$. *Let Y and Z be finite G-sets. Then there exists an isomorphism between G-sets:*

$$C \times W_{C^\perp}[Y + Z, Y] \cong_G W_C[F \times Y + Z, Z].$$

COROLLARY 4.2. *Assume that* $(|G|, q) = 1$. *Let* x, y *be elements of the Burnside ring* $\Omega(G)$ *(or more generally elements of* $\mathbb{C} \otimes_{\mathbb{Z}} \Omega(G)$*). Then*

$$C \times W_{C^\perp}[x, y] = W_C[x + (q-1)y, x - y]$$

in the Burnside ring (or in $\mathbb{C} \otimes_{\mathbb{Z}} \Omega(G)$*).*

As some special cases of the theorem and the corollary, we have the following results.

(1) Taking the cardinalities, we have that

$$|C| \times w_{C^\perp}(y + z, y) = w_C(qy + z, z) \qquad (y := |Y|, z := |Z|)$$

and

$$|C| \times w_{C^\perp}(x, y) = w_C(x + (q-1)y, x - y).$$

Both identities mean the ordinary MacWilliams identity.

(2)In the theorem, let $Y := \mathbf{1}, Z := \emptyset$. Since $W_{C^\perp}[\mathbf{1}, \mathbf{1}] \cong_G C^\perp$ and $W_C[F, \emptyset] \cong_G F^N = V$, we have that

$$C \times C^\perp \cong V.$$

In particular, if C is self-dual, that is, $C^\perp = C$, then $V \cong_G C \times C$, and so $|N/H|$ is even for any subgroup H of G (this result is trivial when $q = 2$ because H is of odd order). To tell the truth, we can take FG-module isomorphisms as these G-set isomorphisms. See the next section.

5. The outline of the proof

In this section we shall state only the outline of the proof. As before, we assume that G acts on $N := \{1, \cdots, n\}$ and that C is a G-code in the row vector space $V := F^N$ over $F := GF(q)$. Furthermore, we assume that $(|G|, q) = 1$. All modules are supposed to be finitely generated.

For $R \subseteq N$, we put

$$\begin{aligned} V(R) &:= \{ v \in V \mid \mathrm{supp}(v) \in R \} \\ &= \{ v \in V \mid v_i = 0 \quad \forall i \notin R \} \cong F^R; \\ C(R) &:= C \cap V(R). \end{aligned}$$

These are F-subspace of V and the following statements hold:

(1) The maps

$$V(-) : R \mapsto V(R),$$
$$C(-) : R \mapsto C(R)$$

are both functors from $(2^N)^{\mathrm{op}}$ to $\mathbf{Mod}_F$, where we regard the G-set 2^N as a category (see Section 3). In other words, $V(-), C(-)$ are F-modules over 2^N. In fact, for $\sigma \in G$ the isomorphism $V(R) \overset{\cong}{\longrightarrow} V(R^\sigma)$ and $C(R) \overset{\cong}{\longrightarrow} C(R^\sigma)$ are given by $v \mapsto v^\sigma$.

(2) Furthermore, there are F-modules over 2^N defined as follows:

$$R \mapsto V, C, C(R)^\perp, C(N-R), V/C(R), C(R)^* (:= \mathrm{Hom}_F(C(R), F)), \text{etc.}$$

(3)As F-subspaces over 2^N of the constant F-module $V : R \mapsto V$ over 2^N,

$$V(R)^\perp = V(N-R), C(N-R)^\perp = C^\perp + V(R).$$

LEMMA 5.1. *(i)* $C^* \oplus C^{\perp}(-) \cong V(-) \oplus C(N-(-))^*$ *as* F*-modules over* 2^N.

(ii) $C \times C^{\perp}(-) \cong V(-) \times C(N-(-))$ *as sets over* 2^N.

PROOF: (i) There are F-isomorphisms as follows:

$$(*) \qquad V/C(N-R)^{\perp} \cong C(N-R)^*$$

$$(**) \qquad C(N-R)^{\perp}/V(R) \cong C^{\perp}/C^{\perp}(R).$$

$(*)$ is clear. $(**)$ follows from the isomorphism theorem and the facts that $C(N-R)^{\perp} = C^{\perp} + V(R)$ and $C^{\perp}(R) = C^{\perp} \cap V(R)$. It is easily checked that these isomorphisms give isomorphisms F-modules over 2^N. Thus (i) follows from Maschke's theorem stated in Section 2. (ii) Let H be any subgroup of G and R an H-subset of N. We put $D := C(R)$, so that D is an FH-module. Since $(|G|, q) = 1$, we have that $D = D^H \oplus [D, H]$, where $[D, H]$ is the subspace of DC generated by $\{ -u + u\tau \mid u \in D, \tau \in H \}$. Thus $|(D^*)^H| = |(D/[D,H])^*| = |D^H|$. By Lemma 2.2, we conclude that $C(-)$ and $C^*(-)$ are isomorphic as sets over 2^N. Thus (ii) follows from (i).

We can now prove the equivariant MacWilliams identity. Let Y and Z be any finite G-sets. The map $(Z+Y)^N \longrightarrow 2^N$; $\rho \mapsto \rho^{-1}(Y)$ is a G-map, and so it can be regarded as a functor between categories. See Section 2. This functor induces a **pull-back functor**

$$[(2^N)^{\mathrm{op}}, \mathbf{Mod}_F] \longrightarrow [((Z+Y)^N)^{\mathrm{op}}, \mathbf{Mod}_F] \,;\, (M(R))_{R \subseteq N} \mapsto (M(\rho^{-1}(Y))_{\rho}.$$

Next, there is a forgetful functor

$$[((Z+Y)^N)^{\mathrm{op}}, \mathbf{Mod}_F] \longrightarrow [((Z+Y)^N)^{\mathrm{op}}, \mathbf{Set}_f] \cong \mathbf{Set}_f^G/(Z+Y)^N.$$

Furthermore, there is a functor which corresponds total spaces:

$$\mathrm{tot} : [((Z+Y)^N)^{\mathrm{op}}, \mathbf{Set}_f] \longrightarrow \mathbf{Set}_f^G \, ; \, (A(\rho))_\rho \mapsto \widetilde{A} := \coprod_\rho A(\rho).$$

Take the composition of these functors, we have the following functor:

$$\omega : [(2^N)^{\mathrm{op}}, \mathbf{Mod}_F] \longrightarrow \mathbf{Set}_f^G.$$

This functor maps the F-module $C(-) : R \mapsto C(R)$ over 2^N to

$$\widetilde{W}_C[Z,Y] := \{ (u,\rho) \in C \times (Z+Y)^N \mid \mathrm{supp}(u) \subseteq \rho^{-1}(Y) \}.$$

By the above lemma, we have that

$$C^* \oplus C^\perp(-) \cong V(-) \oplus C(N-(-))^*$$

as F-modules over 2^N. Their images by the functor ω gives the isomorphisms between G-sets as follows:

$$C \otimes \widetilde{W}_{C^\perp}[Z,Y] \cong_G \widetilde{W}_C[F \times Y, Z]$$

On the other hand, we can easily prove that there exists a canonical G-set isomorphism

$$\widetilde{W}_C[Z,Y] \cong_G W_C[Z+Y,Y].$$

Hence the above isomorphism gives the required isomorphism

$$C \times W_{C^\perp}[Z+Y,Y] \cong_G W_C[Z+F \times Y, Z].$$

6. A WEIGHT ENUMERATOR IS AN INVARIANT POLYNOMIAL

We shall continue to use the notation of the preceding section. For any subgroup H of G, let

$$\varphi_H : \Omega(G) \longrightarrow \mathbf{Z}\,;\, X \mapsto |X^H|$$

be the ring homomorphism defined in Section 2. We put

$$\Omega := \mathbf{C} \otimes_{\mathbf{Z}} \Omega(G).$$

Then the above map φ_H can be extended to $\varphi_H : \Omega \longrightarrow \mathbf{C}$, and furthermore by the fundamental theorem for Burnside rings Ω is isomorphic to $\mathbf{C} \otimes \widetilde{\Omega}(G) = \mathbf{C}^{C(G)}$ by $\varphi := \prod \varphi_H$.

We shall first calculate $\varphi_H(W_C[x,y])$. Let H be any subgroup of G. We decompose N into H-orbits as follows:

$$N_{|H} \cong_H \coprod_i n_i(H_i\backslash H),$$

where $H_1, H_2, \cdots$ are pairwise non-conjugate subgroups of H.

PROPOSITION 6.1. *Let x, y be elements of Ω. Put $x_i := \varphi_{H_i}(x), y_i := \varphi_{H_i}(y)$. Then*

$$\varphi_H W_C[x,y] = \sum_{(r_i)} A^H_{(r_i)} \prod_i x_i^{n_i - r_i} y_i^{r_i},$$

where

$$A^H_{(r_i)} := \sharp\{\, u \in C^H \mid supp(u) \cong_H \sum_i r_i(H_i\backslash H)\}.$$

We define a linear map M by

$$M : \Omega \oplus \Omega \longrightarrow \Omega \oplus \Omega ; \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \frac{1}{\sqrt{q}} \begin{pmatrix} x + (q-1)y \\ x - y \end{pmatrix}.$$

Then it follows easily from the equivariant MacWilliams identity that if C is self-dual, then $W_C[x, y]$ is invariant under M, and so the polynomial of several variables on the right side of the above proposition is also invariant under the transformation $M : x_i \mapsto (x_i + (q-1)y_i)/\sqrt{q}, y_i \mapsto (x_i - y_i)/\sqrt{q}$.

We shall consider binary self-dual codes. We define other linear transformations on $\Omega \oplus \Omega$ as follows:

$$J : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} x \\ -y \end{pmatrix}, \qquad K : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} x \\ \alpha y \end{pmatrix},$$

where α is an element of Ω such that

$$\varphi_D(\alpha) = \sqrt{-1}^{|G:D|} \qquad \text{for all } D \leq G.$$

THEOREM 6.2. *Assume that $q = 2$, G is of odd order and C is self-dual. Then the following hold:*

(1) $W_C[x, y]$ is invariant under the transformations M, J.

(2) If C is doubly-even, that is, the weight of every codeword is a multiple of 4, then $W_C[x, y]$ is invariant under the transformations M, K.

This theorem follows from the above proposition. In particular, using notation in the above proposition, $\varphi_H W_C[x, y]$ is, as polynomial of variables $x_1, y_1, x_2, y_2, \cdots$, invariant under M and $J : x_i \mapsto x_i, y_i \mapsto -y_i$ (or under M and $K : x_i \mapsto x_i, y_i \mapsto \alpha(H_i)y_i$).

LEMMA 6.3. *(1) The group $\Lambda := \langle M, J\rangle$ is isomorphic to a dihedral group of order 16.*

(2) The group $\Gamma := \langle M, K\rangle$ is isomorphic to $\mathbb{Z}_8 * GL(2,3)$, the central product of the cyclic group of order 8 and the general linear group, of order 192.

7. NUMERICAL EXAMPLES

A doubly-even binary self-dual code C has the length n divided by 8 and satisfies the bound for the minimal distance

$$d \leq 4[\frac{n}{24}] + 4.$$

When the equality holds in this inequality, the code is called to be **extremal**. It is a famous open problem whether there exists an extremal doubly-even binary self-dual code of length 72 or not. Let C be such a code of length 72. The weight distribution of this code is uniquely determined by the MacWilliams theorem for ordinary weight enumerators.

$$\begin{aligned}
A_0 &= A_{72} = 1;\\
A_{16} &= A_{56} = 2\,49849;\\
A_{20} &= A_{52} = 181\,06704;\\
A_{24} &= A_{48} = 4629\,62955;\\
A_{28} &= A_{44} = 43973\,42400;\\
A_{32} &= A_{40} = 1\,66027\,15899;\\
A_{36} &= 2\,57567\,21120.
\end{aligned}$$

Other A_r are all 0. It is proved that a prime dividing the order of the automorphism group of C is at most 7, if it exists, by J.H.Conway, J.Thompson, V.Pless , etc. In this section, we shall study C with an automorphism of order 7. But our method does not induce a contradiction and the contracted code is uniquely determined.

After this, C denotes a doubly-even binary self-dual code and G denotes a group of automorphisms of C of order 7. Conway and Pless ([CP82]) proved that N has 2 orbits of length 1 and 10 orbits of length 7.

We shall determine the polynomial $\varphi_G W_C[x, y]$. By Proposition 6.1, we have that

$$\varphi_G W_C[x, y] = \sum_{r_1, r_2} A_{r_1, r_2} x_1^{10-r_1} y_1^{r_1} x_2^{2-r_2} y_2^{r_2},$$

where $x_1 := \varphi_1(x), x_2 := \varphi_G(x), \cdots$, and

$$A_{r_1, r_2} := \sharp\{u \in C^G \mid |u| = 7r_1 + r_2, |supp(u)^G| = r_2\}.$$

This polynomial is invariant under the group $\Gamma := \langle M, K \rangle \subseteq \mathrm{GL}(4)$ of order 192. See Lemma 6.3.

Put $R := \mathbb{C}[x_1, y_1, x_2, y_2]$. We want to know the invariant ring R^Γ. The ring R is a bi-graded as follows:

$$R = \bigoplus_{r,s \geq 0} R_{r,s},$$

where

$$R_{r,s} := \{\sum_{i,j} a_{i,j} x_1^{r-i} y_1^i x_2^{s-j} y_2^j \mid a_{i,j} \in \mathbb{C}\} \subseteq R.$$

Since the Γ-space $R_1 := \mathbb{C}x_1 \oplus \mathbb{C}y_1 \oplus \mathbb{C}x_2 \oplus \mathbb{C}y_2$ is the direct sum of the Γ-subspaces $R_{1,0} = \mathbb{C}x_1 \oplus \mathbb{C}y_1$ and $R_{0,1} = \mathbb{C}x_2 \oplus \mathbb{C}y_2$, we have that

$$R^\Gamma = \bigoplus_{r,s\geq 0} (R_{r,s})^\Gamma.$$

The **Generalized Molien series** is defined by

$$F_\Gamma(\lambda,\mu) := \sum_{r,s\geq 0} \dim(R_{r,s})^\Gamma \lambda^r \mu^s.$$

Then Molien's theorem for the generalized Molien series states that

$$F_\Gamma(\lambda,\mu) = \frac{1}{|\Gamma|} \sum_{\sigma\in\Gamma} \frac{1}{\det(1-\lambda\sigma_1)\det(1-\mu\sigma_2)},$$

where σ_1 and σ_2 are the matrix representations of σ on $R_{1,0}$ and $R_{0,1}$, respectively.

Using a computer, we can calculate the sum of this series.

$$\begin{aligned} F_\Gamma(\lambda,\mu) &= \frac{\lambda^{30}\mu^{30}+\cdots}{(1-\lambda^8)(1-\lambda^{24})(1-\mu^8)(1-\mu^{24})} \\ &= \frac{1+(\lambda+\lambda^{17})\mu+(\lambda^2+\lambda^{10}+\lambda^{18})\mu^2+\cdots}{(1-\lambda^8)(1-\lambda^{24})}. \end{aligned}$$

Now, $\varphi_G W_C[x,y]$ belongs to the subspace $R_{10,2}$. Define the ring

$$S := \mathbb{C}[w_8(x_1,y_1), w_{24}(x_1,y_1)],$$

where

$$\begin{aligned} w_8(a,b) &:= a^8 + 14a^4b^4 + b^8, \\ w_{24}(a,b) &:= a^{24} + 759a^{16}b^8 + 2576a^{12}b^{12} + 759a^8b^{16} + b^{24}. \end{aligned}$$

Here $w_8(a,b)$ is the weight enumerator of the extended Hamming code H_8 and $w_{24}(a,b)$ is the weight enumerator of the Golay code G_{24}. Under these notation, the above result about the generalized Molien series $F_\Gamma(\lambda,\mu)$ implies that $\dim_{\mathbf{C}} R_{10,2} = 2$ and that

$$\varphi_G W_C[x,y] \in Sf_4 \oplus Sf_{12} \oplus Sf_{20},$$

where

$$\begin{aligned}
f_4 &:= (x_1x_2 + y_1y_2)^2,\\
\Delta &:= x_1y_1(x_1^4 - y_1^4),\\
f_{12} &:= \{2x_1y_1(x_2^2y_1^2 - x_1^2y_2^2) + (x_1^4 - y_1^4)x_2y_2\}\Delta\\
f_{20} &:= \{(x_1^3y_2 - x_2y_1^3)^2 + 3x_1^2y_1^2(x_1x_2 - y_1y_2)^2\}\Delta^2.
\end{aligned}$$

Since the minimal distance of C is 16, there is no coefficient of $x_1^9y_1x_2y_2$. By this condition, the polynomial $\varphi_G W_C[x,y]$ is uniquely determined:

$$\begin{aligned}
\varphi_G W_C[x,y] = {} & x_1^{10}x_2^2 + 5x_1^8y_1^2y_2^2 + 10x_1^6x_2^2y_1^4\\
& + 32x_1^5x_2y_1^5y_2 + 10x_1^4y_1^6y_2^2 + 5x_1^2x_2^2y_1^8 + y_1^{10}y_2^2.
\end{aligned}$$

For example, the fact that the coefficient of $x_1^4y_1^6y_2^2$ equals 10 means that there are ten codewords $u \in C^G$ such that $|u| = 7\cdot 6+2$ and $|\mathrm{supp}(u)^G| = 2$, that is, u is of weight 44 and $\mathrm{supp}(u)$ contains the two element set N^G. In particular, putting $x_1 := x_2 := a, x_2 := y_2 := b$, we have the weight enumerator of the contracted code D of C:

$$w_D(a,b) = a^{12} + 15a^8b^4 + 32a^6b^6 + 15a^4b^8 + b^{12}.$$

Thus D is the unique indecomposable self-dual code of length 12.

We want to check the congruence relation. In this case, this condition states that for any element t of $\widetilde{\Omega}(G)$, t is in the image of $\varphi : \Omega(G) \longrightarrow \widetilde{\Omega}(G)$ if and only if $\varphi_G(t) \equiv \varphi_1(t) (\mathrm{mod}\ 7)$. Assume that the variables x, y are are contained in the Burnside ring $\Omega(G)$. Then $x_2 \equiv x_1 \equiv x_1^7 (\mathrm{mod}\ 7), y_2 \equiv y_1 \equiv y_1^7 (\mathrm{mod}\ 7)$. Thus we have that

$$\begin{aligned} \varphi_G W_C[x,y] &\equiv \varphi_1 W_C[x,y] \\ &\equiv x_1^6 + 5x_1^2y_1^4 + 3x_1^2y_1^4 + 4x_1^6y_1^6 + \cdots . \end{aligned}$$

So we can not get a contradiction by this way.

8. Problems

Main Problem. Extend coding theory to coding theory with group action.

In this paper, we considered the MacWilliams identity. To tell the truth, the proof of the equivariant MacWilliams identity in this paper is just a straightforward extension of the proof written in Pless' book.

Exercise. Observe that the proof of the equivariant MacWilliams identity gives a proof of the ordinary MacWilliams identity in the case where $G = 1$. What result does the equivariant MacWilliams identity give in the case where G is a cyclic group and acts regularly on $N - N^G$.

The following sub-problems are important:

(1) Study cyclic codes. A cyclic code is a code with cyclic automorphism group which acts regularly on the coordinates.

(2) Find equivariant versions of various kinds of bounds(e.g., the singleton bound or the sphere packing bound).

(3) Can we prove mass formulas for self-dual codes with group actions.

(4) What can we say about lattices with finite group actions? Can we define the equivariant version of theta functions? There is no Maschke theorem for lattices.

In order to study equivariant coding theory, the following problems are important:

(5) Get a condition that a polynomial map $\widetilde{\Omega}(G) \times \widetilde{\Omega}(G) \longrightarrow \widetilde{\Omega}(G)$ of degree N comes from $\Omega(G) \times \Omega(G) \longrightarrow \Omega(G)$. We might obtain extended congruence relations.

(6) Develop the theory using other Hermite inner products instead of the usual one $\sum_i u_i v_i$. When we consider the decompositions of V and C by central idempotents, such the inner products can appear.

References

[bf Bu11] W.Burnside, "Theory of groups of finite order," Dover, 1955).

[**CS88**] J.H.Conway and N.J.A.Sloane, "Sphere Packings, Lattices and Groups," Springer-Verlag, Berlin-New York, 1988.

[**Di79**] T. tom Dieck, "Transformation Groups and Representation Theory," Lecture Notes in Math., 766, Springer-Verlag, Berlin-New York, 1979.

[**MMS72**] F.J.MacWilliams, C.L.Mallows and N.J.A.Sloane, *Generalizations of Gleason's theorem on weight enumerators of self-dual codes*,

IEEE Trans. Information Theory **IT-18** (1972), 794–805.

[**MS77**] F.J.MacWilliams and N.J.A.Sloane, "The Error-Correcting Codes North Holland, Amsterdam-New York-Oxford, 1977.

[**Pl82**] V.Pless, "Introduction to the Theory of Error-Correcting codes," John Wiley & Sons, New York, 1982.

[**Yo87**] T. Yoshida, *Fisher's inequality for block designs with group action*, J. Fac. Sci. Univ. Tokyo **34** (1987), 513–544.